Information System Security Guidelines
For
Federal, State and Local Agencies
Receiving Electronic Information from the
Social Security Administration

Social Security Administration
Office of Systems Security Operations Management

Version 1.2 March 2003

Information System Security Guidelines for Federal, State and Local Agencies Receiving Electronic Information from the Social Security Administration

1. Purpose

This document provides security guidelines for Federal, State and Local agencies (hereafter referred to as '**outside entities**') that obtain information electronically from the Social Security Administration (SSA) through information exchange systems. The guidelines are intended to assist SSA's information exchange partners to understand the criteria SSA will use when evaluating and certifying the system design used for electronic access to SSA information. The guidelines also will be used as the framework for SSA's ongoing compliance review program of its information exchange partners.

2. Background

A. Legislation

SSA is required by law to protect personal information from unauthorized use or disclosure. Initially, section 1106 of the Social Security Act (42 U.S.C 1306) established SSA's commitment to the confidentiality of information in SSA records even before automated information management systems existed. In 1974, based on the ever-expanding use of automated information systems, Congress enacted the Privacy Act (5 U.S.C 552a) to provide guidance to Federal agencies concerning the collection, use and disclosure of personal information. The Privacy Act requires that public notice be given concerning information maintained in any systems of records. In 1988, the Computer Matching and Privacy Protection Act (P.L. 100-503) amended the Privacy Act to govern computer matching activities between Federal agencies, and between Federal

agencies and State agencies, and requires those agencies to notify individuals before any action can be taken based on matched information. SSA complies with these and other statutes governing personal privacy and has developed system security procedures to prevent unauthorized disclosure of information protected by the Privacy Act by its employees.

B. SSA's Approach to Systems Security

SSA collects and maintains vast amounts of personal information that is needed to carry out its enumeration, earnings record maintenance and benefit program administration responsibilities. This information is managed by a variety of automated information retrieval and support systems comprising SSA's nationwide information management, claims processing and communications infrastructure. Generally, SSA's approach to information systems security involves in-depth analysis of applications and data usage by SSA employees, development of security requirements to address vulnerabilities identified through risk assessment, implementation of controls and full security testing prior to implementation of new systems. SSA designs up-front controls into its systems to minimize opportunity for misuse and maintains vigorous anomaly detection, audit trail and exception reporting mechanisms to alert managers to questionable activity. SSA also conducts ongoing systems security and awareness training for its employees, and maintains a well-defined system of procedures and sanctions for addressing employee misuse of protected information.

C. Role of the SSA Office of Systems Security Operations Management

The SSA Office of Systems Security Operations Management (OSSOM) has agency-wide responsibility for interpreting, developing and implementing security policy; providing security review and integrity review requirements for

all major SSA systems; managing SSA's fraud monitoring and reporting activities, developing and disseminating training and awareness materials and providing consultation and support for a variety of agency initiatives. OSSOM also is responsible for assuring that external systems that receive information from SSA are secure and operate in a manner that is consistent with SSA's own systems security policies, and are in compliance with the terms of information sharing agreements executed by SSA and outside entities. Within the context of these guidelines, OSSOM also is responsible under the Federal Managers Financial Integrity Act (FMFIA) for conducting periodic reviews of third party systems that receive Federal information.

D. Conformity with IRS Guidelines

SSA and the Internal Revenue Service (IRS) share several areas of responsibility for collecting and maintaining earnings and/or self-employment related information for workers. In many cases, this information is considered Federal tax return information subject to the confidentiality and nondisclosure provisions of the Internal Revenue Code (26 U.S.C. 6103). SSA, therefore, is subject to IRS guidelines concerning the use, handling and disclosure of this information.

SSA is required by law to share information, including some Federal tax return information, with certain outside entities that are authorized to use the information in the administration of government benefit programs. The exchange of information occurs most often through the BENDEX and BEER batch data exchanges (see below). Because these systems contain tax return information, outside entities receiving this information from SSA become subject to IRS guidelines concerning the use, handling and disclosure of Federal tax information, as well.

SSA expects its information exchange partners that also receive Federal tax return information to comply with IRS security guidelines (See IRS Publication 1075 (Rev. 1-98), Tax Information Security Guidelines for Federal, State and Local Agencies), thereby establishing a "floor" of security standards for which the IRS conducts its own periodic compliance audits. SSA's system security guidelines apply to the use of information that is outside the definition of Federal tax return information but nonetheless covered by the Privacy Act.

3. SSA Information Exchange Activities

SSA is required by law to provide certain information it collects about individuals to other Federal or State agencies that administer government benefit programs. SSA has a history of providing this information electronically to outside entities, first through batch and/or overnight data exchanges, and more recently, by offering the capability of online access to SSA information.

Following are the electronic information exchanges available from SSA.

Batch/Overnight Exchange

- Beneficiary and Earnings Data Exchange (BENDEX)
- Beneficiary Earnings Record Exchange (BEER)
- State Data Exchange (SDX)
- Enumeration Verification System (EVS)
- State Verification and Exchange System (SVES) (a.k.a., the File Transfer Management System (FTMS))

Online Access

- State On Line Query (SOLQ)

4. Security Guidelines

A. General Systems Security Standards

Outside entities that receive SSA information through online, overnight or batch data transmission must comply with the following general systems security standards concerning the maintenance and control of SSA information. Regardless of the method used to obtain electronic information from SSA, the outside entity must restrict access to the information to authorized employees who need it to perform their official duties. Similar to IRS requirements, information retrieved from SSA data bases must be stored in an area that is physically secure from access by unauthorized persons during both duty and non-duty hours, or when not in use. SSA information will be processed under the immediate supervision and control of authorized personnel. Safeguards must ensure that unauthorized personnel cannot retrieve SSA information by means of computer, remote terminal or other means.

All persons who will have access to any SSA information must be advised of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in the applicable Federal laws. SSA may, at its discretion, make on-site inspections or other provisions to ensure that adequate safeguards are being maintained by the outside entity.

B. Additional System Security Guidelines for Online Access

Outside entities that receive SSA information for online access (i.e. SOLQ) must comply with the following additional guidelines, which consist of requirements that must be met before SSA will approve online access to information and requirements for ongoing monitoring and oversight of online access to SSA information. For this purpose, online access means that an outside entity decides to provide individual users with access to discrete transaction records by way of

a set of online screens or other comparable presentation, rather than limiting access to batch activity (i.e. generated computer listings/printouts). When SSA receives a request to convert batch/overnight access to online access, the entity must comply with the current SOLQ requirements, including the certification process, before online access to SSA information will be approved.

1. System Design Documentation

Outside entities receiving SSA information through online systems access must develop and maintain written documentation of the overall design and security features of their system. This written documentation must be updated any time significant architectural changes are made to the system or to the system's security features. This guideline must be met before SSA will approve the outside entity's request for online access to SSA information, and whenever SSA reviews the outside entity's system for compliance with the terms of their information exchange agreement with SSA.

Meeting this Guideline

Before certifying online access to SSA information, SSA will request a written description of the of the outside entity's system configuration and security features. The written description should include the following:

a. A general description of the major hardware, software and communications platforms currently in use, including a description of the system's security design features and user access control; and

b. A description of how SSA information will be obtained by and presented to system users, including sample computer screen presentation formats; and

c. A description of the organizational structure and relationships between systems managers and users, including an estimate of the number and type of users that will have access to SSA data.

No specific format for submitting this information is required. However, regardless of how it is presented, the information should be submitted over the signature of an official representative of the outside entity. After being certified to receive SSA information online, the outside entity should submit, in writing, to OSSOM a description of any significant changes to the entity's system architecture or security system design. SSA will verify the status of this information and review compliance with this guideline during periodic reviews.

2. Automated Audit Trail

Outside entities receiving SSA information through online access must develop and maintain a fully automated audit trail system capable of data collection, data retrieval and data storage. At a minimum, data collected through the audit trail system must associate each query transaction to its initiator and relevant business purpose (i.e. the client record for which SSA data was requested), and each transaction must be time and date stamped. Each query transaction must be stored in the audit file as a separate record, not overlaid by subsequent query transactions.

Access to the audit file must be restricted to authorized users with a "need to know" and audit file data must be unalterable (read only) and maintained for

a minimum of three (preferably seven) years. Retrieval of information from the automated audit trail may be accomplished online or through batch access. This guideline must be met before SSA will approve the outside entity's request for online access and will be verified periodically during compliance reviews.

Note: Outside entities that receive SSA information through SVES/FTMS also must maintain an audit trail. For SOLQ, the audit trail must be fully automated, including retrieval of individual audit transaction records.

Meeting this Guideline

Prior to being certified for online access, the outside entity must certify, in writing, that their system design for online access to SSA information will include the automated audit trail capability. When certifying the outside entity's system, SSA will select a random sample of transactions received from the outside entity during their development and testing phase, and request a demonstration of the system's audit trail retrieval capability. The outside entity must be able to identify the employee who initiated the online query request for SSA information, the time and date of the request, and the purpose for which the transaction was originated.

Shortly after certification, and during periodic compliance reviews, SSA will verify the automated audit trail capability by asking the outside entity to retrieve audit trail information for a sample of live transactions received by SSA. The information submitted to SSA in support of the sample transactions must be certified as accurate by an appropriate management official of the outside entity.

3. System Access Control

The outside entity must utilize and maintain technological access controls that limit access to SSA information to only those users authorized for such access based on their official duties. The receiving entity must use a recognized user access security software package (e.g. RAC-F, ACF-2, TOP SECRET) or an equivalent security software design. The access control software must utilize personal identification numbers (PIN) and passwords (or biometric identifiers) in combination with the user's system identification code. The outside entity must have management control and oversight of the function of issuing and maintaining access control PINs and passwords to ensure that only authorized users have access to SOLQ.

Meeting this Guideline

Prior to being certified for online access, the outside entity must provide to SSA a written description of their technological access controls, including identifying the type of software used, an overview of the process used to grant access to protected information for workers in different job categories, and a description of the function responsible for PIN/password issuance and maintenance. When certifying the outside entity's system, and during compliance reviews, SSA will meet with the individual(s) responsible for these functions and observe a demonstration of the procedures for logging onto the system for accessing SSA information through the online query.

4. Monitoring and Anomaly Detection

The outside entity's security system must include the capability of monitoring access to sensitive (e.g. celebrities, the organization's own employees, etc.) information, including the capability of detecting anomalies

in the volume and/or type of queries requested, and verifying that each request for SSA information is in compliance with valid official business purposes. The security system must produce reports indicating the capability to appropriately monitor user access, such as:

- User ID exception reports

  This type of report captures information about users who enter incorrect user ID's when attempting to gain access to the system, including failed attempts to enter a password.

- Inquiry match exception reports

  This type of report captures information about users who may be initiating SOLQ transactions for Social Security Numbers that have no client case association within the outside entity's system.

- System error exception reports

  This type of report captures information about users who may not understand or be following proper procedures for SOLQ access.

- Inquiry activity statistical reports

  This type of report captures information about SOLQ usage patterns among authorized users.

The outside entity should have in place procedures for distributing reports to appropriate local managers/supervisors, or to local security officers, to ensure

that the reports are used by those whose responsibilities include monitoring the work of the authorized SOLQ users.

Meeting this Guideline

Prior to being certified for online access, the outside entity must certify, in writing, that their system design for online access to SSA information will include monitoring and anomaly detection capabilities to deter employees from browsing unauthorized information. If available, the outside entity should submit sample report formats to SSA for review. When certifying the outside entity's system, and during compliance reviews, SSA will request a demonstration of this capability and expect to review copies of reports indicating the capability to monitor user access. SSA also will want to meet with employees responsible for reviewing such reports and taking necessary action.

5. **Management Oversight and Quality Assurance**

The outside entity must establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized employees have access to SOLQ and to ensure there is ongoing compliance with the terms of the entity's agreement with SSA. The management oversight function must consist of one or more individuals whose job functions include responsibility for assuring that use of online access to SSA information is appropriate for each employee position type for which SOLQ access is granted. This function also should include responsibility for assuring that employees granted access to SOLQ receive adequate training on the sensitivity of the information, safeguards that must be followed, and the penalties for misuse, and should perform periodic self-reviews to monitor ongoing usage of the online capability. In addition, there should be the

capability to randomly sample work activity involving online requests for SSA information to determine whether the requests comply with these guidelines. These functions should be performed by employees whose job functions are separate from those who request online information from SSA.

Meeting this Guideline

Prior to being certified for online access, the outside entity must verify, in writing, that they will establish and/or maintain ongoing management oversight and quality assurance capabilities for monitoring the issuance and maintenance of user ID's for online access to SSA information. The outside entity should describe how these functions will be performed within their organization and identify the individual(s) or component(s) responsible for performing these functions. When certifying the outside entity's system, SSA will meet with the individuals responsible for these functions and request a description of how these responsibilities are carried out.

6. **Security Awareness and Employee Sanctions**

The outside entity must establish and/or maintain an ongoing function that is responsible for providing security awareness training for employees that includes information about their responsibility for proper use and protection of SSA information, and the possible sanctions for misuse. Security awareness training should occur periodically or as needed, and should address the Privacy Act and other federal and state laws governing use and misuse of protected information. In addition, there should be in place a series of administrative procedures for sanctioning employees who violate these laws through the unlawful disclosure of protected information.

Meeting this Guideline

Prior to being certified for online access, the outside entity must verify, in writing, that they will establish and/or maintain an ongoing function responsible for providing security awareness training for employees that includes information about their responsibility for proper use and protection of SSA information, and the possible sanctions for misuse of online access to SSA information. The outside entity should describe how these functions will be performed within their organization, identify the individual(s) or component(s) responsible for performing the functions, and submit copies of existing procedures and employee acknowledgement statements. When certifying the outside entity's system, SSA will meet with the individuals responsible for these functions and request a description of how these responsibilities are carried out.

7. SSA Certification Review

The outside entity must participate in a review of their security infrastructure and implementation of these security guidelines. SSA will conduct an initial security certification review prior to authorizing the entity's online access to SSA information and a follow-up review after implementation. Generally, the certification review will address each of the guidelines described above and will include, where appropriate, a demonstration of the outside entity's implementation of each guideline. SSA will provide sample transaction data to demonstrate the audit trail capability during the initial review and actual transaction data during the follow-up review. Once certified, SSA will conduct periodic compliance reviews according to the timeframe established by the information sharing agreement with SSA.

Meeting this Guideline

After the outside entity receives approval to enter into an online information sharing agreement, SSA system security personnel will begin assessing the outside entity's ability to comply with these guidelines. The assessment will be based on information submitted to SSA and staff level discussions. When the outside entity is ready to implement online access, they should contact appropriate SSA systems security personnel to schedule the certification review.

The SSA security certification review will consist of a walkthrough of the entity's data center to observe physical security safeguards, a demonstration of the implementation of online access to SSA information, and discussion of each of these guidelines with the outside entity's responsible management personnel. SSA also will request audit trail information for sample

transactions and will visit at least one of the outside entity's field offices to discuss the online capability with workers and managers.

Following a successful security certification review, both parties will sign a document indicating the entity's willingness to comply with these guidelines. Thereafter, the outside entity must participate in a follow-up certification review conducted by SSA after live transmission of online information, and in periodic compliance reviews conducted according to the timeframe established by the information sharing agreement with SSA. The outside entity also must notify SSA of any changes in the systems design, policies, management or security controls upon which access to online information was certified.